**Informative Speech: Paying for What’s Yours**

1. **Introduction**
   1. **Attention Getter:** A virus that makes you pay for the files you created. Imagine clicking on one ad in your browser, or forgetting to update Java, or clicking an email you shouldn’t, and suddenly your midterm paper due tomorrow is locked on your computer and you have to pay a $250 ransom to get it back. This is a reality called ransomware and is on the rise today. From hospitals to home users, it’s targets are indiscriminate.
   2. **Background and Audience Relevance:** Students consistently get infected with viruses due to a variety of reasons, including an inclination towards piracy and visiting suspicious websites. Most of the time they’re not aware of it. Ransomware doesn’t require administrative access, as all it does is open your files, encrypt them (kind of like password protecting) in such a way that they aren’t usable to you, and make you pay for a code to decrypt them. While ransomware is a bit more common in a corporate climate than your house, it only needs to target someone who’s willing to pay to work. For it’s rapid growth, it’s largely understudied by the general public.
   3. **Speaker Credibility:** I’ve worked for almost a year now at The Crypsis Group, a group that largely works with ransomware and the victims of ransomware, and has the somewhat controversial stance of advocating for and facilitating the payment of ransoms. I’ve personally executed and reverse engineered ransomware to determine if a company truly needs to pay, to see how it works, and to prevent future infection.
   4. **Thesis:** Ransomware is a growing trend the general public needs to have a passing knowledge of in order to understand the risks.
   5. **Preview of Main Points:** In this speech, you’ll learn about the effects of ransomware, how it spreads, whether it’s worth to pay it off, and how the payment generally works**.** Understanding how the payment works is important to understand whether it’s worth paying. This is not going to cover safe browsing or malware as a whole, as a good amount of people understand safe browsing, whereas few understand ransomware in particular.
2. **Transition to Main Point:** To start us off, let’s study how ransomware can affect you.
3. **Main Point 1:** Not many have heard of ransomware, but it’s important to know how the typical ransomware works in the event you’re ever affected.
   1. Ransomware has a list of files it deems unimportant, whether that be your MP3 files or Word Documents, that it thinks it can encrypt without damaging your system to the point that you can’t pay your ransom. Once your files are successfully encrypted, it prompts you to pay a Bitcoin address, a cryptocurrency that’s generally untraceable you can buy online at exchanges or even at certain ATMs. There’s even a Bitcoin ATM at the Shell on Chain Bridge Road in Fairfax, but online exchanges are cheaper. Bitcoin is volatile as a currency but one bitcoin is the equivalent of $654 USD today. Bitcoin is not always used as the currency, but it’s the most common and least known currency used to pay ransoms.
   2. Ransomware has a few techniques to try to lock you out. Some don’t let you open browsers, some shut down your antivirus, and some don’t even let you fully boot up your computer. Recently ransomware has closed out programs like Microsoft Word and Browsers just to get access to the files you’re working on presently.
4. **Transition**: Now that you know about ransomware’s functionality, it’s beneficial to understand what to do when it attacks.
5. **Main Point 2**: Ransomware commonly infects the user via a browser or another computer, but for personal use it’s going to come via the web browser 99% of the time. If you are infected, it’s important to weigh if you should pay or not.
   1. **Sub Point 1:** In an interview with Vice President of The Crypsis Group, and my boss, Matt Ahrens, we discussed how generally users aren’t educated to the extent that they don’t understand how to avoid getting infected by malware, so they find themselves affected. Browsers are one of the biggest entry points into a user’s machine. It’s important to keep your browser updated and not click on any suspicious links, as they may trigger dangerous downloads or attempt to exploit any lack of updates. Google Chrome is the most protective of it’s users between Chrome, Firefox, and Internet Explorer and generally leads in cybersecurity, whereas Internet Explorer is very commonly hacked, but they’re looking to remediate that. This is mostly thanks to Google’s elite security team. Most of all, practicing good user behavior is key. Understanding to not click unknown links and to not download/run suspicious or pirated programs is key.
   2. **Sub Point 2:** The FBI and related authorities commonly do not recommend paying ransoms, but this is because paying a criminal is never a good idea in their eyes. Ultimately, it’s a moral question as to whether you’re willing to fund a campaign that put you in this situation because you need your files back. It’s also a matter of whether your data is worth it or not. Sometimes it tells you what you’re missing, but sometimes it doesn’t and masks the filenames, which is why it never huts to fully back up your system before there’s an incident. While Bitcoins can be delivered in fractions, just demanding 2 BTC is over $1000. You wouldn’t pay 1 Bitcoin or $650 just to get your bootleg Yeezus album decrypted, but maybe your company’s work for the past year would be worth it.
6. **Main Point 3:** What can you do to proactively prevent this kind of disaster?
   1. **Sub-point 1:** Keep backups in a regular and available place, and do not actively keep them around as writeable (don’t have a USB plugged into your machine 24/7) as that can just as easily be decrypted. Many companies don’t want to invest in backups and they regret it after the fact.
   2. **Sub-point 2:** Actively educate yourself on ways ransomware, and malware as a whole, spreads and gets onto your system. Update your browser and related software. Update your machine. These updates commonly come with security fixes for the software. Don’t click suspicious links that try to download unwanted content or exploit your browser. Try not to pirate content when you don’t have to because there’s absolutely no guarantee you are getting what you intend to get.
7. **Conclusion**
   1. **Review main Points:** Ransomware is a growing threat and it’s important to know how and why it spreads, and how to remediate it. Browsers are key points of entry into a computer and it’s important to pay careful attention to the security of your browsing. When this fails, it’s a moral question as to whether or not you’d pay.
   2. **Restate Thesis:** Ransomware is a growing trend and as such, the general public needs to understand the risks and remediation associated with this.
   3. **Memorable Closer:** At the end of the day, ethics aside and technology aside, how much are you willing to pay for your own intellectual property?

Gallagher, Sean. "OK, Panic—Newly Evolved Ransomware Is Bad News for Everyone." *Ars Technica*. Ars Technica, 08 Apr. 2016. Web. 25 Oct. 2016.

Goodin, Dan. "Experts Crack Nasty Ransomware That Took Crypto-extortion to New Heights." *Ars Technica*. Ars Technica, 11 Apr. 2016. Web. 25 Oct. 2016.

Wagstaff, Keith. "Big Paydays Force Hospitals to Prepare for Ransomware Attacks." *NBC News*. NBC News, 23 Apr. 2016. Web. 25 Oct. 2016.

Woolsey, Angela. "Fairfax Enters The Growing World of Bitcoin." *Fairfax Times*. Fairfax Times, 29 Oct. 2015. Web. 25 Oct. 2016.